STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS; WILL WE BE READY FOR THE NEXT ATTACK?

BY

LIEUTENANT COLONEL JAMES F. COSTIGAN
United States Army

USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

Information Operations; Will We Be Ready for the Next Attack?

by

James F. Costigan
USA

COL (Ret) Michael Morin
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel James F. Costigan

TITLE: Information Operations; Will We Be Ready for the Next Attack?

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 30 CLASSIFICATION: Unclassified

My thesis is that current doctrine establishes Information Operations in such a way as not to provide clarity on how we conduct operations today, but rather it is serving to muddy waters we're trying to navigate in. Our adversaries of the future will continue to focus along traditional and non-traditional means of attacking us. More emphasis will be placed on rogue and non-state players and their abilities to attack this nation. We can no longer afford to focus on traditional methods of conducting warfare. We must be prepared to fight and win both symmetrical and asymmetrical battles using both kinetic and non-kinetic means. The actions taken to protect and defend this country will require a significant cultural change on the part of the military and the nation. The defense of our nation is not just about protecting our shores against attack. It must include the defense and protection of our national infrastructure.

We are not ensuring that the soldiers, sailors, airman, and marines, as well as civilians in the Department of Defense, are trained properly. Information technology changes rapidly. The warriors that will be required to use it, must have a skill set that is maintained accordingly. That doesn't happen today.

Our strategic leaders must be looking 20 to 25 years down the road when implementing strategies for ensuring that such an infrastructure and all the value it possesses is still viable. They must have a vision that will guide our actions over the next quarter of a century.

We must be open to change. Changes will need to be made in the way we look at Information Operations, the systems we use to fight our future wars, and the way we train our warriors of the future. If we fight this changing environment and the roles that come with it, we risk becoming a force that is irrelevant.

TABLE OF CONTENTS

INFORMATION OPERATIONS; WILL WE BE READY FOR THE NEXT ATTACK?

The attacks on September 11, 2001, resulted in significant loss of life and property. We continually see the faces of those left behind, and hear the stories of the lives of those lost. Plans to rebuild after such a cowardly attack have been prepared and are being executed. But what of the plans to prevent just as deadly an attack in the future? What if the attack is non-kinetic yet has just as devastating an effect, if not greater? What will happen if the power grid for New York City shuts down and can't be brought back up? What do we do if sewage backs up in our streets because the information system used to control it has been hacked and shut off? What will the impact be if all supplies destined for Alaska get routed to Florida and those headed for Florida head to Alaska because someone was able to break into the logistics system and route them accordingly? Ask the same question with a military context to it. That is, what if parts ordered for the Asian Theater are sent to Europe? What if our Global Positioning Systems become inoperable because the satellite network that supports it is no longer available due to an attack? What if our Command and Control systems that we depend on no longer function properly because they've been tampered with? All of the scenarios above pertain to the proper controlling of information and information systems.

Our armed forces have been drastically reduced in numbers since the early 1990's and Desert Storm. Yet we believe we are just as powerful, if not more so, given our use of information technology. We believe that if we have the right information, we can attack any adversary in such a way as to destroy him/her while minimizing friendly and non-combatant casualties as well as collateral damage.

"Information Operations" is the new term we use to combine many of the operations that we have conducted for years. I believe the term has come about given our dependency on information and the emphasis we're placing on using it to make the right decisions. What does the new concept mean to military strategic and operational war-fighters of this nation? That has yet to be determined.

The actions that must be taken to protect and defend this country will require a significant cultural change on the part of the military and, for that matter, the nation as a whole. We can no longer have a work force that is intimidated by computers but rather embrace them fully. We must have industry continue to make operating systems in a much friendlier manner. Also, in the past we have been concerned about protecting our shores against attack. Such a notion today should also include the defense and protection of our national infrastructure. An attack against our infrastructure, though not by an invading force and without physical destruction, is

an attack against the United States. As such we must do what we can to protect that infrastructure so as to be assured of having the appropriate information when we need it.

Our strategic leaders must be looking 20 to 25 years down the road to when implementing strategies for ensuring that such an infrastructure and all the value it possesses is still viable. They must have a vision that will guide our actions over the next quarter of a century. I believe they have done that and will show how, in particular, the Signal Corps' strategic leaders are taking us down the right path.

THE THREAT

There are many foreign states and non-state (terrorist) organizations that would love to see harm come to the United States. They have tools and weapons that we've never fought against. They have intercontinental standoff capabilities that we need to come to grips with. They can bring as much destruction, if not more, with the stroke of a key board, as they can with gun or bomb. Future solutions to this dilemma will involve the close cooperation among many agencies of our government today that are responsible for our national elements of power; diplomatic, informational, military, or economical. For instance, the Federal Bureau of Investigation (FBI) recently issued a warning that Al-Qaida terrorists may be using the World Wide Web to find information about potential targets such as power plants and emergency services systems. The FBI and their National Infrastructure Protection Center (NIPC), works closely with the Department of Defense's Directorate of Information Systems Agency (DISA) to ensure that our nation's vital information infrastructure is protected and available.

The future will find numerous states that pose a threat to our vital interests. A number of them will possess offensive Information Operations (IO) capabilities. One state in particular is China.

China is demonstrating an intense fascination with Information Warfare (IW). Only the United States and Russia rival their analytical work in IW. The potential advances in Chinese doctrine and capabilities have direct implications for U.S. national security.[1]

They are struggling with their national military strategy and their place in the global economy. Information Warfare offers opportunities to win wars without the traditional clash of arms. It could provide China with the capacity to hinder American military operations in the Asia-Pacific, a region of central importance to U.S. national security interests. China recognizes the importance of high technology and the growing power of information in the era of globalization and interdependence. They aspire to become a major political and economic player in a global community where information power retains a critical place in dictating

interstate relations. Given that economic development remains its highest national priority, China's integration into the information-based international economic system has in turn magnified the appeal of information. The ability to compete economically and wage high-technology warfare with information technologies will be critical components of China's national strength. [2]

Information Warfare promises to compensate for China's largely antiquated conventional armed forces. It could enable them to fight from a position of relative military weakness, particularly against far superior military powers like the United States and Japan. It provides potential capacity to reach directly into the American homeland, This has been far beyond the very limited power projection capabilities of China's military. They could attack vulnerable critical infrastructures throughout the world but in particular, the United States to influence or manipulate domestic public perceptions and, in turn, weaken America's political will to intervene or fight. [3]

The tools China could use in their IW doctrine include physical destruction, dominance of the electromagnetic spectrum, computer network warfare, and psychological manipulation. The Chinese also envision "hard" weapons that would physically destroy any enemy's headquarters, command posts, and C2 facilities. The delivery systems include guided bombs, guided artillery shells, cruise missiles, and anti-radiation missiles. They believe the contest for the electromagnetic spectrum to gain battlefield initiative is a crucial phase of warfare. The objective is to dominate the electronic spectrum while denying the enemy's effective use of electronic equipment. Computer warfare can manifest itself in cyber and hacker wars. Virtual warfare as a means to deceive enemy forces with simulated false commands. Psychological warfare and deception involves the transmission of information or misinformation to influence the intended audiences' emotions, mode of thinking, and ultimately their behavior. Aimed at both the military and public as the audience, psychological warfare would exert pressure and weaken the enemy's will to carry on the fight[4]

China will likely devote substantial resources to studying the use of and acquiring state-of-the-art information technologies. Command and control systems, such as reconnaissance satellites and surveillance systems will become important elements in China's force structure. It is, however, unclear how they might apply newly acquired IW capabilities. This level of uncertainty on when and how China would master IW adds greater urgency to understanding Chinese strategic thought on IW.[5]

China recognizes that they are likely to fight from a position of weakness. Given that, they'll seek to achieve political objectives while precluding an actual clash of arms that would

likely result in defeat. This concept dovetails closely with Sun Tzu's dictum of winning without fighting and Mao's people's war concept of overcoming the superior with inferior forces.

Hackers, while considered the enemy by some, have provided us with a very valuable service. For years there was a group of them that had told us (those that would listen) that our systems were vulnerable. No one listened. They've made us listen and they were right. That's probably why many firms have hired them on as security experts. Having said that, we must find a way to protect our information infrastructure from them as well. Hackers kept themselves and system administrators very busy during the year 2001. We saw a 200% increase in computer security incidents and vulnerabilities this past year. There were more than 52,000 incidents including web attacks, malicious viruses, and network intrusions reported to the Computer Emergency Response Team (CERT), the federally funded computer security clearinghouse at Pittsburgh's Carnegie Mellon University. The number for 2001 accounted for more than half the attacks since 1988, which was the first year the CERT began keeping records.[6]

How do we protect ourselves as well as take the fight to any adversary that dares to face us? The answer may be asymmetric methods of war fighting such as Information Operations.

This nation and the Army in particular, will fight today and tomorrow's war in a much different fashion than those of previous generations. The American public expects her military to fight and win wars while at the same time minimizing casualties. A senior defense official is quoted as saying in December of 2000, "We used to worry about losing. Now we worry about winning perfectly." [7] Desert Strom established this standard and we have proven that we are capable of achieving it over the last nine years. Perhaps Sun Tzu said it best, "Generally, in battle, use the normal force (direct approach) to engage; use the extraordinary (indirect approach) to win".[8]

Our forces today are reliant upon information to fight and win our wars. We are so reliant upon it that I would wage to say that it is our strategic center of gravity. Center of gravity is defined as, "Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight". [9]If we lose our ability to gather accurate information, our forces will be at risk given the evolving doctrine of today. In order to continually meet the American public's expectations, Joint Force Commanders will be required to formulate and execute plans based on solid information gathered from sources inside and outside of the traditional military structure. They must operate in an environment that achieves and maintains Information Superiority. Information Superiority (IS) is "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while

exploiting or denying an adversary's ability to do the same".[10] The evolution of information technology will increasingly permit us to integrate the traditional forms of information operations with sophisticated all-source intelligence, surveillance, and reconnaissance in a fully synchronized information campaign. The development of a concept labeled the global information grid will provide the network-centric environment required to achieve this goal. The grid will be the globally interconnected, end-to-end set of information capabilities, associated processes, and people to manage and provide information on demand to war-fighters, policy makers, and support personnel.[11]

Joint Vision 2020 is based on being able to achieve the operational concepts of Dominant Maneuver, Precision Engagement, Focused Logistics, and Full Dimension Protection.[12] None of these concepts are possible without the critical enabler of Information Superiority. Napoleon once said, "To guess at the intention of the enemy, to divine his opinion of yourself, to hide both your intentions and opinions, to mislead him by feigned maneuvers, to invoke ruses, as well as digested schemes, so as to fight under the best conditions—this is and always was the art of war".[13] The word "superiority" implies a state or condition of imbalance in one's favor. Information superiority is transitory in nature and must be created and sustained by the joint force throughout the conduct of information operations."[14]

INFORMATION OPERATIONS

The Joint Force Commander (JFC) directs three interdependent contributors to achieve Information Superiority (IS). They are Intelligence, Surveillance, and Reconnaissance (ISR), Information management (IM), and Information Operations (IO) to include its related activities.[15] I will only focus on IO.

Joint Publication 1-02 defines Information Operations as "those actions taken to affect an adversary's information and information systems while defending one's own information and information systems." [16] It also includes actions taken in a non-combat or ambiguous situations to protect one's own information and information systems as well as those taken to influence target information and information systems. The joint force commander conducts information operations whether facing an adversary during a conflict or engaged in humanitarian relief operations. Such operations will be synchronized with those of multinational and interagency partners as the situation dictates. The commander may also employ non-kinetic weapons, particularly in the arena of Information Operations where the targets might be key enemy leaders or troop formations, or even the opinion of an adversary.[17]

Information Operations are either offensive or defensive in nature. Offensive Information Operations are the integrated uses of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decision makers or to influence others to achieve or promote specific objectives.

Defensive IO is the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. Defensive IO ensures timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes.[18] Four interrelated processes comprise defensive IO: information environment protection, attack detection, capability restoration, and attack response. Offensive actions play an integral role in the defensive process in that they can deter adversary intent to employ IO and/or neutralize adversary capabilities.[19]

United States Army Field Manual (FM) 3-0, dated June 2001, identifies twelve Army IO elements. They are Operation Security (OPSEC), Psychological Operations (PSYOP), Counterpropaganda, Military Deception, Counter-deception, Electronic Warfare (EW), Computer Network Attack, Physical Destruction, Information Assurance (IA), Physical Security, Counterintelligence, and Special IO. There are also two related communities that must be synchronized with IO. They are Public Affairs (PA) and Civil-Military Operations (CMO). For this reason, there are those that feel the definition is too broad. In fact, if you look at again, you'll see there isn't anything that IO doesn't cover. Does that mean all operations are Information Operations? A white paper dated 11 July 2000 from the Joint Staff put it simply, "Combining all of these definitions, it becomes apparent that current joint doctrine allows for virtually any military operation to be termed an "information" operation, thus calling into question the concept's uniqueness and usefulness. [20] I agree. However this could serve as a topic for a strategic research paper by itself. For that reason I will move on.

Many argue that the central point of IO is Information Technology while others argue it's the information itself that is critical to successful IO. The answer is both.

The first part of the answer lies not in today's environment of stove piped systems throughout a given command center, but rather in a network-centric one that provides the supported systems a venue to operate over. The information systems network enables the JFC to successful wage his/her campaign. It must be properly installed, operated and maintained. The soldiers, sailors, airman, and marines that operate it, must be trained continually. Without this blend of technology and individual, those systems attached to the network will provide no utility to the commander.

The second part recognizes that the commander or soldier on the ground that knows more about his/her enemy, that can affect what their enemy knows or thinks they know, and can put the appropriate force and munitions on a target, has the advantage. They also have the ability to minimize casualties because they can make more timely and educated decisions. This is where the term "Decision Superiority" comes into play. Information superiority is only part of the equation. If smart decisions aren't made based on the data available, it's all been for naught. Two quick historical references may help. In September of 1944, the Allied leadership in World War II was planning the largest airborne assault of its day. It was called Operation Market Garden. Intelligence sources via the underground and aerial photography had identified armor forces stationed in the city of Arnhem, which was to be the objective. The leadership failed to take advantage of the intelligence provided to them and the operation failed. December of 1944 provides a somewhat similar example. The allied leadership had inaccurately defined the disposition of the German forces that they faced. They believed they were beaten and on the verge of giving up. If they had the proper information, they would have figured out Adolf Hitler's intent of counterattacking through the Ardennes forest and positioned their forces appropriately. This intelligence failure resulted in the needless loss of lives.

Information provides the Joint Force Commander a competitive advantage only when it is effectively translated into superior knowledge and decisions. The joint force must be able to take advantage of superior information converted to superior knowledge to achieve decision superiority - better decisions arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission.[21] It results from superior information filtered through the commander's experience, knowledge, training, and judgment; the expertise of supporting staffs and other organizations; and the efficiency of associated processes. Decision superiority does not automatically result from information superiority. Organizational and doctrinal adaptation, relevant training and experience, and the proper command and control mechanisms and tools are equally necessary.[22]

WAR FIGHTING PROCESS

Our war-fighting Commander-in-Chiefs (CINCs) have the best in information technology to assist them in fighting our nation's wars. However, we still lack the infrastructure at the operational and tactical levels that will allow them to utilize it. More specifically, the amount of bandwidth (the size of the pipe that information flows through) is not enough to support the new systems being used. Air Force Major General Charles E. Croon, Vice Director for Command

and Control Communications and Computer systems, recently said that, "It's always bandwidth. The demand always outruns the capacity".[23] Our problem is that we speak about being a Joint organization out of one side of our mouth, yet out of the other we are very armed service (Army, Navy, Marine Corps, and Air Force) oriented. The communications field is a classic example of where the DOD must give the joint staff the authority and resources to establish specific DOD-wide standards, and ensure that those standards are adhered. Why does each of the armed services have their own communication systems? There should only be one standardized system across the entire Department of Defense. This concentrated effort may result in systems that provide the CINCs with the necessary bandwidth that they need.

Joint Force Commanders must synchronize all the information available to them so as maximize its utility. There is a process whereby CINCs integrate IO targets into the overall targeting plan via the Joint Target Coordination Board (JTCB). Information Operations targets, like others, require joint and interagency coordination.

Joint Force Commanders must have legitimate and legal targets to pursue in order to successfully complete their mission. An integral part of the deliberate and crisis planning process is the IO cell. The IO officer works for the J-3. He/she ensures IO is implemented per the JFC's guidance. The IO serves as the JTCB IO cell representative. In a perfect world the cell consists of representatives from each of the J-staff sections. At a minimum, the IO must work with counterintelligence, public affairs, legal, and civil affairs representative.

The Joint Task Force conducts IO in coordination with other military commands and agencies. They can include the Joint Staff, the National Security Agency, the Defense Information Systems Agency, law enforcement, the Defense Intelligence Agency, other federal agencies, Non-Government Organizations (NGO), and International Organizations. Close coordination is required to ensure everyone's operations are synchronized and the desired end state is achieved. Non-DOD United States government departments and agencies may have a role in the planning and accomplishment of IO. The IO officer must ensure that non-DOD department and agencies that have on-going programs and interests in the joint area of operation are consulted in the development of IO plans. The concerns of multinational forces and governments should also be considered when appropriate.

The Civil-Military Operations Center (CMOC) is suited for ensuring coordination is achieved prior to targets being presented to the Joint Target Coordination Board. Joint Pub 1-02 defines the CMOC is an "ad hoc organization, normally established to assist in the coordination of activities of engaged military forces, other United States agencies including a local US Embassy, NGO, private voluntary organizations, and regional and international

organizations. There is no established structure, and its size and composition are situation dependant."[24]

Information Operations targets can include civilian, military, social and cultural leadership as critical elements of a given civilian infrastructure. These may be legitimate targets but, at the same time, may do more harm to friendly forces when they are destroyed. For instance, destruction of a water facility may be a military advantage, but that advantage is minimized if it destroys the water supply for the towns-people as well.

Information Operations officers must be integral members of the team. They can save lives by achieving objectives without killing anyone. They must be innovative in their approach to mission accomplishment; always looking at the big picture, not just the military.

As noted earlier, our nation's information systems are in constant danger of being attacked. These systems enable us to implement our national elements of power. These elements fall into the categories of diplomatic, informational, military, and economic means of national power. Over the past ten to fifteen years, industry has been more concerned with getting new products out into the market, then making sure that they are secure. Thus we have systems in our economic, political, military, and information infrastructures that are in danger. This leads us to the concept of Information Assurance (IA).

Joint Publication 1-02 defines IA as "Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."[25] Threats to information systems include physical destruction, denial of service, capture, environmental damage, and malfunctions. Information Assurance provides an enhanced degree of confidence that information and information systems possess the following characteristics: availability, integrity, authentication, confidentiality, and non-repudiation.

Much of the information that a Joint Force Commander utilizes is gained from resources beyond his/her control. Information from other governmental agencies, International Organizations and Non-Governmental Agencies will often prove to be very valuable. The synchronization of this information will have an impact on the plans and tactics that he/she will utilize. Having said that, the Joint Force Commander must be taught that information systems need to be maintained, and protected. Information security is not a static concept. It is difficult to achieve and arguably more difficult to maintain. The adversaries of tomorrow will continue to make smarter bombs and we must be continually on the lookout. Perhaps an analogy would help explain the point. Years ago, one of the first inventions to come out after the law

enforcement community introduce the radar gun for speed control, was the "fuzz buster". It enabled a driver to detect when a radar gun was being used; giving them ample opportunity to slow down. We see that today in the Information Technology world where viruses, and hoaxes that are designed to disrupt and destroy systems are deployed, detected, and defeated. The adversary then develops a stronger, more lethal, and harder to break virus next time.

TRAINING, PEOPLE, CULTURE, AND CHANGE!

All the systems in the world with all the right policies for using them won't solve our problem if we don't educate the folks that use them. Our people are the most important component of securing our systems. Some divide cyber-security into two parts. One part deals with all the technological issues. The other is the human side of this problem. Anyone that ignores the latter is doomed to failure. Ira Hobbs from Government Computer News brings up some very good points in his editorial from the 4 February 2002 issue. He states, " A successful program to improve security has to include robust education so people have the information they need to protect personal and system data". He goes on to say, "...employees must be individually aware of the risks and their personal roles in mitigating them. They need skills to take precautions."[26]

TODAY'S ENVIRONMENT

President George W. Bush continues to guide this nation in its war on terrorism. He has recognized that the adversaries of tomorrow will fight across the entire spectrum of conflict. They will utilize symmetrical methods of war via armored and infantry forces trained to physically fight and destroy targets. He knows that we face a continuing threat from those that will use asymmetrical methods as well. He has picked two individuals to assist him in his fight. They are General (retired) Wayne Downing and Mr. Richard Clarke. General Downing headed the entire United States Special Operations Command. Mr. Clarke, who worked in the administrations of Bill Clinton, Ronald Reagan and Mr. Bush's father, was named special adviser to the president for cyberspace security. Mr. Clarke became national counter-terrorism coordinator at the Clinton White House where he was considered abrasive and secretive. But he was nonetheless respected for his ability to get things done, and he has been watching Osama bin Laden for years. He also warned for years about terrorist attacks, but could get few people to listen.[27]

The President is also making technology protection and innovation a priority in his most current budget. The budget proposal would more than double the growth of federal technology spending. Government information technology spending is slated to reach $52 billion in fiscal

2003 under Bush's budget, up from $48 billion this year. That includes dedicating more than $4.2 billion to cyber-security and a $722 million homeland security effort to improve federal agencies' ability to share information across jurisdictions. The budget proposal includes $23 million for the State Department for a passport modernization system, which aims to decrease the percentage of fraudulent domestic passports. The Department of Justice would get $30.7 million for an integrated automated fingerprint identification system. But most of the increase would be in the Department of Defense as it fights the war in Afghanistan. Defense Department information technology spending would hit $26 billion in 2003, up from $23 billion this year. The government's cyber-security budget alone would increase more than 50 percent, from $2.7 billion to $4.2 billion, under the budget. Every federal agency was required to conduct a computer security assessment and include the cost of updating its systems before the Office of Management and Budget would approve its budget requests.[28] This investment in critical resources shows that the President understands the utility of information technology in protecting our nation from those that wish it harm. It also shows that he has the vision to see that we must protect these systems from any adversary that would aim to prevent us from using them. It postures us to exist in an environment where we have free access to critical information at any time. Information is quickly becoming our strategic center of gravity and we must do what is necessary to ensure its availability.

The war on terrorism, like other fights we've been in, is one that will, more than likely, be fought with international cooperation. The President has indicated a willingness to go it alone, but reality will dictate that we need to fight as a coalition if we want long lasting success. The JFC must have the ability to evaluate information in its multinational context.[29] Technological developments that connect the information systems of partners will provide the links that lead to a common relevant operational picture and improve command and control. However, the sharing of information needed to maintain the tempo of integrated multinational operations also relies heavily on a shared understanding of operational procedures, compatible organizations, and a common understanding of planning processes. The CINCs of today have created numerous relationships where such information is being shared. In particular, CINC United States Pacific Command has reached out to numerous nations in his area of operation and established training programs that teach other nations' military leaders, our deliberate planning process. This understanding of the way we do planning, has created an opportunity where information sharing exists more so today than ever before. There is a risk, perhaps, in setting up such relationships. After all, our friend today, may be our adversary tomorrow. However, the benefits of openness and sharing of our techniques with our friends is worth the risk.

ROLE OF STRATEGIC LEADERSHIP

We live in the Information Age. How we decide to live in it is key to the Army's future. The Chief of Staff and Secretary of the Army have recognized the vital role that information technology will play in executing the transformation of today's Army to a "... strategically responsive force that is dominant across the full spectrum of operations."[30]

I am an Army Signal Corps officer and will confine my argument to the role that can be played by strategic leadership of our Army's Signal Corps. The roles of the Signal Corps and its strategic leaders in the Army of today and the future are critical. Lieutenant General (LTG) Peter Cuviello is the Army's G6 (formerly the Directorate of Information Systems for Command and Control Communications and Computers (DISC4)) and Chief Information Officer (CIO). He and his staff have been actively engaged in developing strategy and plans to support General Shinsheki's vision of Army transformation. Mr. Dave Borland, Deputy Chief Information Officer (CIO) for the Army says, "The entire Army leadership sees information technology across all areas as an absolutely critical enabler of transformation."[31] LTG Cuviello's vision of "A transformed Army with agile capabilities and adoptive processes, powered by world class, network-centric access to knowledge, systems, and services interoperable with the Joint environment" supports the Secretary and Chief's concept of Army Knowledge Management (AKM) which is being dubbed the "The Strategic Transformer". Army Knowledge Management combines the activities of knowledge sharing, technology exploitation, and process improvement. The result is intended to be improved capabilities, increased effectiveness and efficiency, and a faster more accurate decision cycle and streamlined processes.[32]

There are five goals with metrics for AKM listed in the policy memorandum dated 8 August 2001 by the Secretary, and Chief of Staff of the Army. Those goals are to adopt governance and cultural changes to become a knowledge-based organization, integrate knowledge management and best business practices into Army processes, manage the info-structure at the enterprise level, establish Army Knowledge Online (AKO) as the enterprise portal, and prepare personnel for functioning in a knowledge organization by providing learning opportunities.

Goal one indicates that new policies, management structures, and strong leadership at all echelons will be necessary to manage knowledge and info-structure at the enterprise level. Effective October 1, 2001, all Major Commands (MACOM) Information Technology initiatives, other than those that are centrally managed acquisition programs, will be reviewed by the Army CIO Executive Board. Major Command automation funds programmed for information technology efforts will be withdrawn and centrally managed. Each MACOM will immediate curtail information technology investments unless they have a waiver and funding from the Army

CIO. [33] This major shift of policy will be very difficult to implement. In order for it to work, the leadership will have to convince the community that they can provide automation in a timely manner, and capable of meeting commander's needs. The defining of requirements such as to what level do you provide automation, will be a huge challenge. Will Army centralized funds pay for systems down to company level? If not, and a commander wants to, how do they acquire it? Can they acquire it without breaking regulations? The answer lies in recognizing computers as an end item on unit authorization documents. I know of no TOE/MTOE that identifies computers on them. I'm not referring to ULLS boxes and other Army programmed systems. I'm referring to the ones for the commander, senior NCOs, subordinate officers, etc. The Table of Distribution and Allowances (TDA) situation is much worse.

Goal two seeks to establish collaborative environments and find innovative ways of doing business to improve the Army decision-making and operations. The Army will adopt many of the commercial based services being provided to the public today.[34]

Goal three designates a single authority to operate and manage the Army's info-structure at the enterprise level starting with the Military District of Washington not later than 1 February 2002. [35] Our IT networks are operational 24 hours a day, seven days a week. Yet there is no single agency we can point to today that is responsible for maintaining it. The U.S. Army Signal Command, a two-star command, headquartered at Fort Huachuca, Arizona will be tagged to take on this mission. This is long overdue and vital to our survivability in the Information Age. At the same time however, it puts an operational commander, with world wide responsibility to support numerous joint commands and agencies, under the control of the Army G6. They should be a part of a Joint Command and Control Communications operational command. The closest thing to such an organization is the Defense Information Systems Agency (DISA). Among the fundamental benefits gained from such a command would be the enforcement of the Joint Technical Architecture (JTA) established by the J6 of the United States Joint Staff. The JTA identifies standards that are to be enforced when acquiring and utilizing automation. There must be an agency assigned the responsibility of enforcing established standards both from an architectural and individual user's perspective.

Goal four establishes the AKO as the enterprise portal by having every soldier, active duty, Army National Guard, and Army Reserve, and Department of Army Civilian registered to the portal by 1 October of last year. The portal will be upgraded to enable soldiers to do many more things than today.[36] For instance, they will be able to review their personnel files including evaluation reports and awards. A by product of this is going to be a workforce that is much more user friendly with automation systems.

Goal five stresses that the Army is people. We need to provide them with the learning opportunities, career-building tools, and mentoring relationships to improve their value to the Army and the nation.[37] I agree but also believe that the Army has to look seriously at the average age of the civilian work force. If we are to stay competitive and up to date, we need young, enthusiastic employees that are eager to learn and fresh out of college or technical schools. I've been in positions where the average age of the IT workforce was above 50 years old. These are great people, but the IT world of today calls for individuals with a different tool kit. We need a cyber protection force. It must not be in a constant position of catch-up. Rather, they must have the tools and skills to keep us ahead of any adversary we may face. We don't do that with kinetic capabilities and we certainly can't afford to do it with those responsible for the systems that our tanks, artillery tubes, and other weapons systems rely on. The individual must understand that IT is not just electronic mail. They will need to understand how navigate the world wide web, how to tunnel down through systems and segregate the important information from all the data that is out there on the internet. The young soldiers and officers coming into our military have such a familiarity with automation. Their leaders may not. The leaders of our force must understand capabilities that IT can bring. Data transfer, video teleconferencing, satellite and fiber optic communications should be concepts that each war-fighter embraces. You can't grasp that concept if you're afraid of it.

ACADEMIA'S ROLE

The cry for more computer security specialists within the government has not gone unheard. The National Science Foundation has attempted to fix the problem via numerous programs. One such program is the Cyber Corps scholarship program. As early as June of 2001, certain academic institutions were granted millions of dollars for scholarships to individuals that are willing to study computer security and follow up their studies with a stint as a government employee. The first of these universities were University of Tulsa ($2.8 million), Iowa State University ($2.6 million), Carnegie Mellon University ($2.5 million), Purdue University ($2.4 million), Naval Postgraduate School ($2.3 million), and University of Idaho ($1.4 million). [38] Most recently, George Washington University's Ashburn, VA institute has also been recognized for its computer security program. It has established an accelerated, six-month computer security certification program for Information Technology professionals. The curriculum covers the right topics; e-commerce security, information policy, and viruses and worms. The intent is not to further the population of hackers currently causing problems. Rather, the intent is further

the population of information security professionals. They will be the ones fighting the cyber wars of the future.[39]

The National Science Foundation is not the only agency looking to strengthen our information security professional posture. The National Security Agency has recognized Norwich University, the nation's oldest private military institute, for its Bachelor of Science program in Information Assurance and Security Technology. The university will also be eligible for scholarship dollars to support their program.[40]

These are good programs. However, we must find a way to expand the program to include active duty military, both enlisted and officers. At the same time we must find the resources to establish incentives for these individuals to stay and serve their country. These include not only wages, but a program with continuing education as a foundation. Some will argue that the costs are too much for such a program. I will use an idea from a recent commercial to say it best. A program that certifies individuals in cyber security will cost X dollars. The costs for trained systems administrators will be X dollars. The cost for replacing computers and upgrading information infrastructure will cost X dollars. The satisfaction of knowing that your information is safe, accurate, and always available is priceless. We cannot afford to let the program lose its momemtum.

THE ROLE OF CONGRESS

The United States Senate has also stepped up to the plate in an attempt to fix this serious dilemma. Senator John Edwards, a democrat from North Carolina, has sponsored the "Cyber-security Preparedness Act".[41] The intent of the bill is to establish the United States Government as model for Information Security. A companion bill is the "Cyber-security Research and Education Act" which seeks to conduct postgraduate research as well as create a virtual university for Chief Information Officers. [42]

Each of the programs will carry with them a significant cost. I believe that if we could have identified the costs of preventing the tragedy of 11 September 2001, we would have paid them gladly. The same is true for these programs. Having said that, it's not to far fetch to say, that 11 September 2001 would have happened anyway because as Americans, we tend not to believe such things could happen to us. I hope we don't hit that mentality in this very important area.

WE MUST CHANGE; BUT CAN WE?

The Army Knowledge Management way of executing our job is a huge change to our normal means of doing business. A comparison of this change and John P. Kotter's "Eight-

stage process for creating major change"[43] shows a close linkage to stages one through four. Stage one calls for "Establishing a sense of urgency". [44] We cannot continue to operate the way we are and feel secure about our networks. Security, management, and procurement processes need to dramatically change over the next few years. Stage two calls for "Creating a guiding coalition"[45]. That coalition consists of the Secretary of the Army, the Chief of Staff, and LTG Cuviello and their staffs. Stage three calls for "Developing a vision and strategy"[46]. Both the Chief of Staff and LTG Cuviello have created visions that are desirable and clearly understood. The policy memorandum mentioned earlier serves as the initial strategy. It has been developed with objectives (ends), a course of action (ways) and resources (means). Stage four calls for "Communicating the change vision. [47] Whether it is through e-mail that is currently circulating, interviews with professional journals, speaking engagements, or the newly updated AKO web page, the vision is being communicated. When you consider that the policy has just been signed in the Pentagon, and word has reached the foxhole already, it's a pretty significant accomplishment. It's too early to determine success or failure in complying with the policy. My gut feeling is that we're off to a good start.

The real challenge lies in steps five through eight. If action isn't seen, then buy-in will be very difficult. As an example, more and more organizations are out-sourcing the information technology function. As a result, there is a lot of doubt in the government information technology professional family pertaining to this issue. If the part of the strategy that calls for professional development of the work force goes unfulfilled, it will have a significantly negative impact on the accomplishment of the plan. Any short term wins must be communicated and linked to the overall strategy immediately or folks will see it as another whim by the current person in the hot seat.

The next 20 to 25 years will require significant changes to our culture of today. Information systems and the products they produce will become more and more important. Information and our ability to use it correctly will become our strategic center of gravity. Traditional combat systems of today will give way to new ones of the future that will be heavily dependant upon automation technology. The armed forces of the future will be required to turn in their blinders of today and think outside the box to fight and win our nation's wars with the weapons of tomorrow. An example of this can be seen in the extreme hesitancy on the part of the armor battalions at Fort Lewis, Washington that were told to turn in their tanks as part of the Army's transformation process. They same was seen by the light infantry fighters from the infantry battalions in the second brigade that was to go through the process. Those brigades

today have very competent and comfortable leaders and soldiers that understand the value of what the information combat systems they use provides to them.

We face many threats today that we never would have thought of ten years ago. "Code Red", "The Love Bug", and "Melissa" were a football defense, a Disney movie, and a great song by the Allman Brothers. Now they are engraved in my mind as being evil events that represent what could be just the beginning of the threats that our nation and our children face for tomorrow. The AKM initiative has set the conditions for us to start the journey down the road to being more productive and more protected in our Information Age society. We have a good plan. But like all plans that get executed, we need to keep our eyes on the deep as well as close targets that lie ahead and adjust as needed. It will be difficult in the short term, but the benefits down the road will be worth it.

CONCLUSION

The world that we live in today will continue to change dramatically over the next ten to twenty-five years. Traditional threats from countries such as North Korea and Iraq will continue to exist. We will need to maintain forces that have the capabilities to deal with them decisively. Conflicts with these traditional foes will not likely have an impact on our homeland though it's not out of the realm of the possible. Foreign states like China and terrorist organizations such as Al-Qaida will continue to develop asymmetric capabilities that will have the ability to strike the United States in its homeland. They will also seek to establish global instability when it is to their advantage. We must continue to monitor Chinese development of IW doctrine while at the same time monitor their acquisition of information technology that could be used against the United States. Also, dialogue with China and sharing of technology will facilitate stability in the region. Constant vigilance is the only answer to avoiding ugly surprises. China's evolving attitudes toward IW could pose an unpredictable challenge for America.

Investment of the United States taxpayer has been planned for and must be carried out. Upgrading the critical information infrastructure that we use today is essential. Our focus must be on security vice customer service, which has been the case in the past. This will need to be done continually as new ways of attacking information systems are developed. This will require a commitment on the part of the services to ensure information is available to the Defense Department as well as the American public. If we secure our national information infrastructure then we minimize the IW threat of state and non-state players attacking the United States and her interests.

The concept of Information Operations must be continually trained, refined, and resourced in order to take full advantage of what it can do for us on the battlefield of tomorrow.

We must develop strategies that consist of the appropriate ends, ways, and means that will ensure that our critical infrastructure is protected against any attack while at the same ensuring that we possess the ability to take the Offensive IO and any other implementation of our national elements of power, to any adversary that might consider attacking the United States. In order to do this we need talented professionals that are trained in cyber security. These people will play essential roles in ensuring that we have access to the necessary information technology that the Department of Defense and the nation as a whole are relying upon. The world of academia has stepped up to the plate. Their commitment must be continually supported. The Cyber Corps scholarship program should be expanded to provide the same opportunities to our military cyber security forces.

Our culture must change. We've committed ourselves to organizing our businesses, military, government, and lives around information and the smart use of it. We can no longer afford to have a workforce that is afraid of technology. Nothing cures fear better than education. Educate them.

Our senior leaders have developed a vision and strategy for implementing it. We must have faith in its implementation and pass the torch to a younger, more Information Age savvy generation to carry us through the middle to late 21st century.

The Information Age brings incredible potential to this world. We must ensure that it is harnessed to our advantage and not to any adversary's.

Word Count = 7,886

ENDNOTES

[1] Toshi Yoshihara, Chinese Information Warfare: Phantom Menace Or Emerging Threat? , Strategic Studies Institute, U.S. Army War College, Carlisle, PA, November 2001. pg vi

[2] Ibid, pg 6

[3] Ibid, pg 15

[4] Ibid, pg 16

[5] Ibid

[6] Brian Krebs, Computer Security Vulnerabilities Double IN '01 CERT, 14 January 2002, available from http://www.elcom.co.uk/news_story.asp?id=873 ; Internet; accessed 22 January 2002

[7] Mellissa Applegate, Studies in Asymmetry, Preparing for Asymmetry As Seen Through The Lens Of Joint Vision 2020, Strategic Studies Institute, U.S. Army War College, Carlisle, PA, September 2001, pg 1

[8] Department of Defense, Joint Doctrine for Information Operations, Joint Publication 3-13, Washington, DC: U.S. Department of Defense, 9 October 1998, I -1.

[9] Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02,Washington, DC: U.S. Department of Defense, 12 April 2001, pg 63.

[10] Department of the Army, Field Manual (FM) 3-0, Operations, Chapter 11, (Washington, D.C.: U.S. Department of the Army, June 2001). Pg 11-2

[11] Department of the Army, U.S. Army War College, Department of Military Strategy, Planning, and Operations, Information Operations Primer, 2nd edition, January 2002, pg 2

[12] Director for Strategic Plans and Policy, J5, Strategy Division, Joint Vision 2020, (US Government Printing Office, Washington, DC: Department of Defense, June 2000), pg 4

[13] Department of the Army, Field Manual (FM) 3-0, Operations, Chapter 11, (Washington, D.C.: U.S. Department of the Army, June 2001), pg 11-2

[14] Department of the Army, U.S. Army War College, Department of Military Strategy, Planning, and Operations, Information Operations Primer, 2nd edition, January 2002, pg 3

[15] Department of the Army, Field Manual (FM) 3-0, Operations, Chapter 11, (Washington, D.C.: U.S. Department of the Army, June 2001), pg 11-5

[16] Department of Defense, Dictionary of Military and Associated Terms, Joint Publicatoin 1-02 (Washington, DC: U.S. Department of Defense, 12 April 2001) pg 203.

[17] Department of the Army, U.S. Army War College, Department of Military Strategy, Planning, and Operations, Information Operations Primer, 2nd edition, January 2002, pg 3

[18] Department of the Army, Field Manual (FM) 3-0, Operations, Chapter 11, (Washington, D.C.: U.S. Department of the Army, June 2001). page 11-17

[19] Department of the Army, U.S. Army War College, Department of Military Strategy, Planning, and Operations, Information Operations Primer, 2nd edition, January 2002, pg 6

[20] Chris A. Pilecki, Deputy Director for Operations, Information Operations (J-39), White Paper, Getting Our Arms Around Information Operations , 11 July 2000.

[21] Department of the Army, U.S. Army War College, Department of Military Strategy, Planning, and Operations, Information Operations Primer, 2nd edition, January 2002, pg 2.

[22] Ibid

[23] Dawn S. Onley, "Joint Chiefs: Bandwidth is top IT need in Afghanistan", Government Computer News, 21 January 2002, pg 34

[24] Department of Defense, Dictionary of Military and Associated Terms, Joint Publicatoin 1-02 (Washington, DC: U.S. Department of Defense, 12 April 2001) 70.

[25] Department of Defense, Dictionary of Military and Associated Terms, Joint Publicatoin 1-02 (Washington, DC: U.S. Department of Defense, 12 April 2001) pg 202

[26] Ira Hobbs, "Employees could be the weakest security link", Government Computer News, 4 February 2002, pg 35

[27] Elisabeth Bumiller, Bush Picks 2 for Senior Post in the War Against Terrorism, 10 October 2001, available from http://www.nytimes.com/2001/10/10/10BUSH.html ; Internet; accessed 10 October 2001.

[28] Renae Merle, *Washington Post*, Bush Budget Would Boost Technology Spending, Federal Contractors Likely to Benefit, February 5, 2002; Page E01

[29] Ibid

[30] Dennis Steele, "The Army Magazine Hooah Guide to Army Transformation", The Army Magazine, February 2001, pg 21

[31] Dawn S. Onley, "IT Goal is a Quicker, Tougher Army", Government Computer News, 13 August 2001, pg 24

[32] Author not specified, "Vision for Army Knowledge Management, from https://www.us.army.mil/akm/ , accessed 17 August 2001

[33] Peter Cuviello, Lieutenant General, "Road Map for Army Knowledge Management" dated 8 August 2001, from the 1001 Annual Army Acquisition Workshop, from http://www.army.mil/vision/default.htm , accessed 5 April 2002.

[34] Ibid

[35] Ibid

[36] Ibid

[37] Ibid

[38] William Jackson, "NSF awards Phase 1 of cyber-scholarships" Government Computer News, June 18, 2001; Vol. 20 No. 15, pg 46

[39] William Jackson, "GWU battle lab trains IT professionals in security", 21 January 2002, Vol 21, No 2,

[40] William Jackson, "Norwich U. Introduces INFOSEC Degree", Government Computer News, "In brief", 4 February 2002,.

[41] William Jackson, "Bill Calls for Cyber-Security Best Practices", Government Computer News, 4 February 2002, pg 7

[42] Ibid

[43] John P. Kotter, Leading Change. Harvard Business School Press, 1996, pg 21

[44] Ibid

[45] Ibid

[46] Ibid

[47] Ibid

BIBLIOGRAPHY

Applegate, Melissa, Studies in Asymmetry, Preparing for Asymmetry As Seen Through The Lens Of Joint Vision 2020, Strategic Studies Institute, U.S. Army War College, Carlisle, PA, September 2001.

Author not specified, "Vision for Army Knowledge Management, from https://www.us.army.mil/akm/ , accessed 17 August 2001.

Bumiller, Elisabeth, Bush Picks 2 for Senior Post in the War Against Terrorism, 10 October 2001, available from http://www.nytimes.com/2001/10/10/10BUSH.html ; Internet; accessed 10 October 2001.

Cuviello, Peter, Lieutenant General, "Road Map for Army Knowledge Management" dated 8 August 2001, from the 1001 Annual Army Acquisition Workshop, from http://www.army.mil/vision/default.htm , accessed 5 April 2002.

Department of the Army, U.S. Army War College, Department of Military Strategy, Planning, and Operations, Information Operations Primer, 2nd edition, January 2002.

Department of the Army, Operations, Field Manual (FM) 3-0, Washington: U.S. Department of Army, June 2001.

Department of Defense, Joint Doctrine for Information Operations, Joint Publication 3-13, Washington: U.S. Department of Defense, 9 October 1998.

Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02, Washington: U.S. Department of Defense, 12 April 2001.

Director for Strategic Plans and Policy, J5, Strategy Division, Joint Vision 2020, US Government Printing Office, Washington, DC: Department of Defense, June 2000.

Hobbs, Ira, "Employees could be the weakest security link", Government Computer News, 4 February 2002.

Jackson, William, "NSF Awards Phase 1 of Cyber-Scholarships" Government Computer News, June 18, 2001; Vol. 20 No. 15.

Jackson, William, "GWU Battle Lab Trains IT Professionals in Security", 21 January 2002, Vol. 21, No 2.

Jackson, William, "Bill calls for Cyber-Security best practices", Government Computer News, 4 February 2002.

Jackson, William, "Norwich U. Introduces Infosec Degree", Government Computer News, 4 February 2002.

Kotter, John P., Leading Change. Harvard Business School Press, 1996.

Krebs, Brian, Computer Security Vulnerabilities Double IN '01 CERT, 14 January 2002, available from http://www.elcom.co.uk/news_story.asp?id=873 ; Internet; accessed 22 January 2002.

Merle, Renae, *W*ashington Post Staff Writer Tuesday, February 5, 2002, Bush Budget Would Boost Technology Spending, Federal Contractors Likely to Benefit.

Onley, Dawn S., "Joint Chiefs: Bandwidth is top IT need in Afghanistan", Government Computer News, 21 January 2002.

Onley, Dawn S., "IT goal is a quicker, tougher Army", Government Computer News, 13 August 2001.

Pilecki, Chris A., Deputy Director for Operations, Information Operations (J-39), White Paper. Getting Our Arms Around Information Operations , Washington: Department of Defense,11 July 2000.

Steele, Dennis, "The Army Magazine Hooah Guide to Army Transformation", The Army Magazine, February 2001.

Vasishta, Preeti, Matt McLaughlin, and Patricia Daukantas, "Now you see it ...", Government Computer News, 4 February 2002.

Yoshihara, Toshi, Chinese Information Warfare: Phantom Menace Or Emerging Threat? , Strategic Studies Institute, U.S. Army War College, Carlisle, PA, November 2001.